Akamai
Experience the Edge
Quick thinker? Prove it.
#AkamaiCrackTheCode

RISK

1/14/2020
09:30 AM

Kelly Jackson Higgins
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login
50% 50%

Like
Tweet
Share

Industrial Control System Features at Risk

How some ICS product functions can be weaponized by altering their configurations.

A new analysis of industrial control systems (ICS) running in the networks of oil and gas, power generation, refining and chemicals, pulp and paper, and mining industries sheds light on how some legitimate and deeply rooted product features and functions can actually threaten their security.

In many cases, these purpose-built functions embedded in systems can be exploited by malicious attackers by merely changing easily adjusted configurations and settings; malware isn't necessarily required to do so, according to Mark Carrigan, chief operating office of PAS Global. Carrigan's firm studied some 10,000 of its customers' ICS systems to pinpoint features that he describes as "delicate by design" with easily abused configuration capabilities.

It's a spin on the well-known "insecure by design" issue associated with these systems: Security vulnerabilities as well as the lack of security controls in the design of many OT products have been the subject of research for some time. But Carrigan points out that some product features, too, can easily be reconfigured and weaponized.

Not only do many of these systems predate today's cyberthreats, but some of the security-challenged features were built into the systems to make engineers' jobs easier and so they could perform their tasks quickly, according to Carrigan. They can't easily be updated, and even removing some of these weaknesses can, in many cases, cause a ripple effect of disruption in the system and production.

ADVERTISEMENT. CLICK FOR SOUND.

Replay
AUTOMOX
Learn More

While sophisticated or potentially damaging attacks on ICS networks to date have been relatively rare and difficult to pull off without knowledge of a plant's processes as well as the ICS systems within it, security experts say nation-state attackers, via cyber espionage campaigns, are increasingly gaining knowledge to sabotage a plant's operation via a cyberattack. Stuxnet was the first wakeup call for the industrial sector. Most recently was Triton/Trisis, which in 2017 shut down the safety instrumentation system at a petrochemical plant in Saudi Arabia.

Understanding the processes beneath the control systems could be a deadly combination for a malicious hacker able to change the configuration of the OT assets, Carrigan says. "That's the next landscape for attackers," he says.

'Tip of the Iceberg'

Carrigan won't name names of the affected vendors PAS found in its analysis, but some of the exposed features span multiple brands of OT equipment. Of the 10,000 industrial systems, there were some 380,000 total known vulnerabilities with published CVEs, most of which were Microsoft Windows-related. He will present his findings next week at the S4x20 ICS security conference in Miami.

"This is just the tip of the iceberg. There are tons of these out there," Carrigan says.

Dale Peterson, CEO of Digital Bond, a control systems research and consulting firm that runs S4, says Carrigan's study provides another level of insecure-by-design issues. Specifically, some of them include features that are required for components to communicate. To actually fix these issues would entail simultaneously upgrading a large number of components and weeks of production outage, he explains.

"Also, many of these 'features' are hidden or known only to the team deploying the ICS," Peterson notes.

Many of the security-challenged features PAS is highlighting are well-known by the vendors in question, according to Carrigan. Most of the fallout he has seen with those features so far has been with mistakes and inadvertent misconfigurations by the operators themselves, not malicious hackers.

One feature that spans all vendors' control systems products is a parameter or setting generally known as the output characteristic. This control function parameter is a binary setting that determines, for example, the flow rate of air or gas in a valve. If the flow controller is set for 100 and the current flow is 80, it will open the valve to reach 100, for example, he says. "If I just reverse that setting — just switch it ... it's a simple thing to do — that valve opening is going to close. I've [then] reversed the action of the output characteristic," he explains.

Another feature specific to one vendor's control system product — which it recently patched — is a command in the human machine interface's (HMI) graphics files that could allow an attacker to gain administrative control of the entire DCS network, Carrigan says. This feature is for engineers or designers to create a command for an operator, but if an attacker got hold of it, he or she could land admin privileges. It even bypasses any set Windows admin privileges, he says.

Sponsored Content
Optimizing your Managed Security Services Provider
You'll get the most out of your MSSP after a frank discussion about your infrastructure needs and processes.
Brought to you by Raytheon Intelligence & Space

An additional feature at risk is an HTML weakness in most HMIs built in the past 10 years, according to PAS's findings. These HMIs use a free format of HTML for graphics design, according to Carrigan. "If you have HTML, you can inject code and do almost anything you want — change flow control settings, no problem. Do SQL injections in the configuration database, no issue there," he says.

PAS also found a setting in one vendor's control system for balancing computing loads for a flow-control indicator process. By "mixing up" the calculations of the flow indicator and the flow controller on the CPU, an attacker could wreak havoc on the operation. "There's nothing in the system to prevent you from setting those things wrong. So at a minimum I can cause production problems by changing a bunch of these settings," or even overload the CPU, he says.

Another "delicate" feature they found: one vendor's ICS system that uses a single, hard-coded system engineer username and password that is stored in its configuration database. The password is hashed, but Carrigan says it's a very simple and guessable hash. "Once I've [the attacker] figured it out, I know for every single system, I can access that hash and access that system," he explains. The password can't be changed because it's "designed into" the product.

Damon Small, technical director of the NCC Group, says the threat model has changed significantly for the ICS sector, and attacks are becoming more common. But the real-world impact of making security changes like patching or other moves that take operations offline even for a short period of time often deter any major security changes by operators. Small says once when he recommended an operator to patch monthly for Windows flaws, the operator told him that taking those systems offline for just four hours would cost his organization $350,000 in outage time.

"Operators know very well the inefficiencies introduced when you start messing with control systems," Small explains.

What to Do

How do OT operators protect their plants from their own systems, especially if patching may be off the table in some cases?

Adopting configuration management, especially for the most critical systems and assets, is one way to thwart an attack via "delicate" features, according to Carrigan. That way only the changes you allow can take place, for instance, he says.

Passive network monitoring can also catch anomalous traffic and behavior, notes NCC Group's Small, who is also a founding member of the Operational Technology Cyber Security Alliance. "If you see something other than what you were expecting, that could an indicator of something having gone wrong. But this assumes you understand what your normal traffic looks like — what your baseline is," he notes, which requires analysis.

Related Content:

- Siemens Offers Workarounds for Newly Found PLC Vulnerability
- Triton/Trisis Attacks Another Victim
- Industrial Safety Systems in the Bullseye
- Lessons From The Ukraine Electric Grid Hack

DARKReading
NEW
The EDGE

Check out The Edge, Dark Reading's new section for features, threat data, and in-depth perspectives. Today's top story: "6 Unique InfoSec Metrics CISOs Should Track in 2020."

Kelly Jackson Higgins is the Executive Editor of Dark Reading. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise ... View Full Bio

Recommended Reading:

- Startup Aims to Map and Track All the IT and Security Things
- 10 Years Since Stuxnet: Is Your Operational Technology Safe?
- MITRE Engenuity Announces ATT&CK Evaluations for ICS Vendors
- Ripple20 Malware Highlights Industrial Security Challenges

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts
- SecDevOps: Tying Security to Your Application Development Processes
- [Dark Reading Virtual Event] Your Crash Course on Cyber Attackers

MORE WEBCASTS

White Papers
- The Best Free Vulnerability Management Tools
- When and How to Best Leverage an MSSP

MORE WHITE PAPERS

Reports
- 2020 Threat Hunting Report
- Connecting the Dots: Key strategic opportunities in a post-COVID-19 world

MORE REPORTS

Cyber Attackers' Favorite
EXPLOITS
And How to Stop Them
REGISTER NOW
DARKReading VIRTUAL EVENT
Thursday, November 12, 2020 • 11:00 AM ET

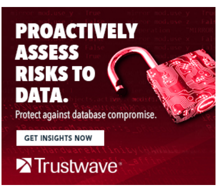
COMMENTS
NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Be the first to post a comment regarding this story.

Related Content Sponsored by Trustwave

RESOURCES | BLOG | VIDEO | TWITTER

- **7 Experts on Transforming Your Threat Detection & Response Strategy** Download the eBook for expert advice on transforming your threat detection and response strategy.
- **IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment** See who IDC lists as top Worldwide Managed Security Services leaders
- **Five Ways Attackers Get to Databases** Download top five ways attackers target your databases
- **The Threat Hunt That Uncovered Novel Malware** See how a threat hunt uncovered novel malware that evaded EDR technologies
- **Best Practices for Database Security in the Cloud** Download this whitepaper to learn about best practices for database security in the cloud.



PROACTIVELY ASSESS RISKS TO DATA.
Protect against database compromise.
GET INSIGHTS NOW
Trustwave

HOT TOPICS | EDITORS' CHOICE

Overcoming the Challenge of Shorter Certificate Lifespans Mike Cooper, Founder & CEO of Revocent, 10/15/2020	2
US Counterintelligence Director & Fmr. Europol Leader Talk Election Security Kelly Sheridan, Staff Editor, Dark Reading, 10/16/2020	1
7 Tips for Choosing Security Metrics That Matter Ericka Chickowski, Contributing Writer, 10/19/2020	1

SUBSCRIBE TO NEWSLETTERS

WEBINARS

- SecDevOps: Tying Security to Your Application Development Processes
- Using Artificial Intelligence, Deep Learning and Machine Learning for Cyber Defense
- The Best Ways to Stop Malware and Ransomware That No One Else Will Tell You

WEBINAR ARCHIVES

WHITE PAPERS

- Cloud Threat Report: Spring 2020
- The Best Free Vulnerability Management Tools
- When and How to Best Leverage an MSSP
- 7 Experts on Transforming Your Threat Detection & Response Strategy
- Self Service Secure Software Design

MORE WHITE PAPERS

DARKReading VIRTUAL EVENT
November 12, 2020
11:00am - 5:00pm ET
Cyber Attackers' Favorite
EXPLOITS
And How to Stop Them
REGISTER

VIDEO

SPIF: An Infosec Tool for Organizing Tools
0 COMMENTS

Supporting Women in InfoSec
0 COMMENTS

ALL VIDEOS

CARTOON

"I'M YOUR HUSBAND, I DIDN'T THINK I NEEDED TO USE MULTIFACTOR AUTHENTICATION."

Latest Comment: I'm done with Technology tonight. The bed won't go up so I'm using pillows, the Kindle is locked up so I'm reading an actual book and ...

CARTOON ARCHIVE

CURRENT ISSUE

DARKReading
Computing's New Normal

Special Report: Computing's New Normal

This special report examines how IT security organizations have adapted to the "new normal" of computing and what the long-term effects will be. Read it and get a unique set of perspectives on issues ranging from new threats & vulnerabilities as a result of remote working to how enterprise security strategy will be affected long term.

DOWNLOAD THIS ISSUE!

BACK ISSUES | MUST READS

FLASH POLL

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

○ Yes
○ No
○ No but we are considering it
○ Still waiting for cybersecurity guidance from Trump admin EO
○ Don't know
○ Other (Please explain in the comments)

Submit

ALL POLLS

REPORTS

DARKReading REPORTS
How IT Security Organizations are Attacking the Cybersecurity Problem
HID

How IT Security Organizations are Attacking the Cybersecurity Problem

The COVID-19 pandemic turned the world -- and enterprise computing -- on end. Here's a look at how cybersecurity teams are retrenching their defense strategies, rebuilding their teams, and selecting new technologies to stop the oncoming rise of online attacks.

DOWNLOAD NOW!

Special Report: Understanding Your Cyber Attackers	0 COMMENTS
2020 State of Cybersecurity Operations and Incident Response	0 COMMENTS
The Changing Face of Threat Intelligence	0 COMMENTS

MORE REPORTS

TWITTER FEED

DarkReading Retweeted

Interop
@interop

In this exclusive training presented by @DEVOPSINST attendees can earn the #DevSecOps Foundation Certification following the course. This course explains how #DevOps security practices differ from other security approaches. View the course description: ow.ly/I6Wb50BWBt5

DevSecOps Foundation Certification Training
NOVEMBER 10, 2020
Learn the purpose, benefits and concepts of DevSecOps including DevOps security strategies and business advantages.
presented by
DevOps INSTITUTE
InteropDIGITAL
LEARN MORE

10h

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2020-5790**
  PUBLISHED: 2020-10-20
  Cross-site request forgery in Nagios XI 5.7.3 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link.
- **CVE-2020-5791**
  PUBLISHED: 2020-10-20
  Improper neutralization of special elements used in an OS command in Nagios XI 5.7.3 allows a remote, authenticated admin user to execute operating system commands with the privileges of the apache user.
- **CVE-2020-5792**
  PUBLISHED: 2020-10-20
  Improper neutralization of argument delimiters in a command in Nagios XI 5.7.3 allows a remote, authenticated admin user to write to arbitrary files and ultimately execute code with the privileges of the apache user.
- **CVE-2020-25157**
  PUBLISHED: 2020-10-20
  The R-SeeNet webpage (1.5.1 through 2.4.10) suffers from SQL injection, which allows a remote attacker to invoke queries on the database and retrieve sensitive information.
- **CVE-2020-25648**
  PUBLISHED: 2020-10-20
  A flaw was found in the way NSS handled CCS (ChangeCipherSpec) messages in TLS 1.3. This flaw allows a remote attacker to send multiple CCS messages, causing a denial of service for servers compiled with the NSS library. The highest threat from this vulnerability is to system availability. This flaw...

Copyright © 2020 Informa PLC Informa UK Limited is a company registered in England and Wales with company number 1072954 whose registered office is 5 Howick Place, London, SW1P 1WG.